In the Specification:

Please amend the title as follows:

DOCUMENT VERIFICATION USING JURISDICTIONAL INFORMATION TO EXTRACT A DIGITAL WATERMARK

At page 13, please amend paragraph 48 as follows:

[48] A digital watermark may carry virtually any type of information associated with a given identification document. This can be especially advantageous with new technologies for the creation of machine readable data. For example, consider technology such as a bar code containing embedded particles (e.g., nanoparticles), as described in an article entitled, "Nanoparticles May Help Fight Fraud," in [~~an online article of~~] NATURE magazine, dated October 30, 2003 [~~and found at http://www.nature.com/nsu/031027/031027-7.html~~]. In this technology, each barcode line contains atoms of permalloy (an iron-nickel mixture), where the printed lines arranges these magnetic particles in unique patterns, each pattern having a measurable, unique magnetic field. This nanoparticle material can be used on areas such as the barcodes of identification documents (or on other parts of the identification document) and a quantitative measurement of the unique magnetic pattern can be taken and encoded as a machine readable signature. For example, the nanoparticle material can be used as a coating on all or part of an identification document, creating a unique machine readable magnetic signature that can then can be stored in a data carrier on the identification document itself (e.g., encoded into a KINEGRAM, stored on a smart card chip, encoded into a digital watermark, stored in an external database, etc.), and encrypted, if desired. Later, during authentication, the unique machine readable magnetic signature information stored about the nanoparticle material can be retrieved and compared with a reading from the location(s) of the actual nanoparticle material, to check the authenticity of the identification document.

At page 23, after paragraph 23, please insert Appendix A as follows:

Appendix A

This Appendix A was written as a direct response to AAMVA's request to provide the best possible "common security device" for use in all DL jurisdictions. Digimarc ID Systems' recommendation is a specially designed Kinegram properly placed within the DL document. Our response is tailored to the individual criteria listed in the AAMVA document.

Overview

The decision by the UID task force to implement a single identifying feature into all DL's is an extremely important and momentous move that will bring an easily recognizable security feature to all licenses in these United States. While a common feature will greatly enhance the ability to authenticate licenses from any jurisdiction, it will also present a large and enticing target for counterfeiters worldwide. Herein lies the basic conundrum or challenge to all of us who have a vested interest in maintaining the security of the country.

On the one hand, it is vital to have a device imbedded in all cards that everyone can immediately identify with a driver's license and that everyone will be able to use, regardless of individual capability, to authenticate the document. On the other hand, we will require that this device can not be easily counterfeited and that its cost will be affordable across all jurisdictions. As with all security devices, this balance is an extremely difficult one to manage. In the end, it takes another point of force to tip the balance in one's favor. This "other point of force" we believe to be AAMVA's ability to combine all jurisdictions procurement power so that the total measure of these United States can be brought to bear in the volume versus cost economic tug and pull reality.

Each of AAMVA's criteria will be addressed separately below:

1. The Device should be available from Multiple Vendors.

Logic is well served in assuring that the technology utilized is available from multiple vendors to assure the absolutely critical requirement of ready and continued supply for years to come. To choose a device available from only one vendor makes the automatic assumption that the vendor chosen will survive through all of the financial climatic

conditions and that the monopoly created might unintentionally be used to the vendor's advantage.

Kinegrams are manufactured by several companies who have been in the business of supplying highly secure features to governments for many years. The technology is in use in many European countries as one of the primary means of securing their Identity Documents. These companies only supply governments and secure companies that deal only in the business of supplying governments. The designs created for individual countries are then forever guaranteed to be for use only in that country or government. No design duplication or near duplication is allowed.

2. The device should be affordable.

The balance of low cost with high security we believe to be one that is only adjudicated under the stress of high volume. That is to say that an individual jurisdiction (or any company) that strives towards a device with an ultra high security level will find that the cost of such a device is high in low or modest volume. The only remedy for this situation is to somehow channel the volumes of all jurisdictions into a single and very large volume demand. Once accomplished, the impossible task of procuring high security at low cost will have been accomplished. Just as the power of our country derives from the combined strength of all of the States, this goal is achieved by combining individual State demands.

Costs of kinegrams are highly volume dependent. The creation of an AAMVA designed master would be the first task. From this master then, all States could derive their own sub-master while maintaining the design features that characterize the original AAMVA design. The way in which kinegrams are manufactured will allow for multiple sub-masters to be used each contributing to the total demand. So, although each State will have its own design, the overall easily identified design will be present. Additionally, the demands from each State will be counted (whatever the size) into the total demand. The total demand determines cost. The cost to each State would be the same regardless of the States particular volume.

By combining all States' demands through one organization, we believe a reasonable cost will be obtained for all jurisdictions.

3. The common device should protect against the threat of counterfeiting/simulation.

Kinegrams have been used for years around the world to secure National ID's of numerous countries. They meet the threats described in the draft of "ISO Standard for International Driver License".

For example, kinegrams offer some unique capabilities that prevent counterfeiting attempts and aide in easy authentication. They can not be photocopied since they are an advanced OVD.

Kinegrams offer absolute color change over a wide range of colors. They give abrupt and absolute shift in colors which can be used as part of the verification process. The fact that a wide range of colors are available speaks to their wide capabilities in satisfying the range of design differences one is bound to encounter State to State.

Kinegrams offer another unique ability in that one can construct letters, numbers, or shapes where viewed in one orientation one part of the letter, etc is dark and the other is light. Then, in an orientation 180 degrees to the first, the dark shifts totally to light and light shifts to dark. For example, the letter A in a simple example could be constructed in such a way that the outside of the A is light and the inside of the A is dark. Then, when the orientation is changed 180 degrees by turning the card half way around, one finds that the outside is now dark and the inside in now light. A similar thing can be made to happen with designs of all types.

Each viewing angle of the kinegram produces vivid visual affects in addition to the affects described above. In this instance, the kinegram acts as a high quality hologram. The virtue here is the easily detected characteristic.

These features together protect against counterfeiting/simulation since they can not be duplicated by simple holograms. One has to create a kinegram to duplicate or simulate a kinegram. The equipment and skill level required to do so are huge barriers to counterfeiting attempts.

4. The device must be easy to locate and easy to interpret.

As stated in the previous section, interpretation and authentication are particularly easy with a kinegram. These are brilliant OVD's and attract attention immediately. The placement on the card in a particular location for all States is highly recommended. Further, the location should coincide with variable data on the card in such a way as to

protect against photo swap or demographic data manipulation by either intrusion or simulation.

The kinegram can be AAMVA designed in such a way as to be immediately recognized as an "official design". It should be designed and constructed to simply and easily allow authentication by absolute color shift and by the light to dark and dark to light shifts described earlier. Other "hologram like" image to image features are also desirable. The kinegram can also contain "laser readable" data (about 64 bits) hidden within the design. These "readable" data inclusions are characteristic only of kinegrams. Additionally, a digital watermark can be incorporated within the graphic design which will be readable with the additional DWM's embedded within the card itself. By embedding the DWM in the common verifier one accomplishes the task of tying the OVD to the State of Issuance and to the card itself which provides an increased level of authentication. These are enhancements available to kinegrams that are not available in other features. The incorporation of a covert / machine readable feature within the common verifier is extremely powerful especially if it ties the feature to the card and locks the total data and graphic packages together.

5. The device should be difficult to anyone other than the jurisdiction's motor vehicle administration to produce.

Because companies that supply kinegrams have developed only by supplying governments and companies that supply governments, this mandate is met in full. Many European countries subscribe to this technology to secure their documents. To our knowledge, there have been no occasions where kinegrams have been successfully simulated/counterfeited.

Again, the master design is frozen and will not be duplicated for any other entity including other government entities. The success and survival of kinegram producing companies depends upon this very notion.

If then, the device is present and in its proper format, it can only reasonably have been placed there by the issuing authority.

6. The particular implementation or design or the device should not be available to anyone but the motor vehicle administrations.

As stated earlier, the technology has been in use for some time in numerous countries around the world. This is tried and true technology and as such is recognized around the world as a truly first class security technology. Each and every country utilizing this technology has designed specific and characterizing designs pursuant to their own needs and desires. Each one has been and remains unique.

AAMVA designs will also be unique. Additionally, the design must be such that the individual States can have the requisite authority within the master design to inject their own individualism. In this way, the overall design identifies it as a US issued document and further modification will identify the specific State. All designs become "locked in designs" and as such are only available to the particular jurisdiction.

7. Adaptable to both central and over-the-counter issuance.

Digimarc ID Systems has done the engineering work necessary to ensure that kinegrams are able to be successfully incorporated into both centrally issued documents (eg – Teslin based cards) and over-the-counter cards (PVC, Composite, and Teslin based OTC cards). It is vital to note that any security device must be designed in such a way as to allow incorporation without compromising the functional properties/characteristics of the card. For example, flex performance, bend radius tolerance, exposure to light, heat, and humidity can not cause either the device to suffer or cause the card to deteriorate. The card, with the common verifier embedded in it, must remain as durable as it was without the device. Card architecture should never be compromised by the inclusion of a security feature.

The properly designed and constructed kinegram can be incorporated within all card types in use today across the United States increasing overall security adding authentication without compromising card durability or field life expectancy.